

(Indicate page, name of
newspaper, city and state.)Page 52
NEWSWEEK MAGAZINEDate: 9/20/99
Edition: Final

Title: "MOONLIGHT MAZE"

Character: 288A-CI-68562
or
Classification:
Submitting Office: Cincinnati

Indexing:

(Mount Clipping in Space Below)

'we're in the middle of a cyberwar'

RUSSIAN HACKERS MAY HAVE PULLED OFF WHAT COULD BE THE MOST DAMAGING BREACH EVER OF U.S. COMPUTER SECURITY

BY GREGORY VISTICA

IT'S BEING CALLED "Moonlight Maze," an appropriately cryptic name for one of the most potentially damaging breaches of American computer security ever—serious enough for the Department of Defense to order all of its civilian and military employees to change their computer passwords by last month, the first time this precaution has ever been taken en masse. The suspects: crack cyberspooks from the Russian Academy of Sciences, a government-supported organization that interacts with Russia's top military labs. The targets: computer systems at the Departments of Defense and Energy, military contractors and leading civilian universities. The haul: vast quantities of data that, intelligence sources

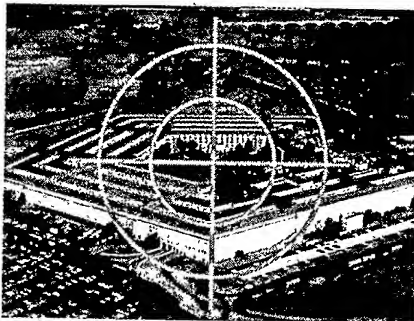
familiar with the case tell NEWSWEEK, could include classified naval codes and information on missile-guidance systems. This was, Pentagon officials say flatly, "a state-sponsored Russian intelligence effort to get U.S. technology"—as far as is known, the first such attempt ever by Russia. Washington has not yet protested to Moscow. But Deputy Secretary of Defense John Hamre, who has briefed congressional committees on the investigation, has told col-

leagues: "We're in the middle of a cyberwar."

In a cyberwar, the offensive force picks the battlefield, and the other side may not even realize when it's under attack. Defense Department officials believe the intrusions, which they describe as "sophisticated, patient and persistent," began at a low level of access in January. Security sleuths spotted them almost immediately and "back-hacked" the source to computers in Russia. Soon, though, the attackers developed new tools that allowed them to enter undetected (although they sometimes left electronic traces that could be reconstructed later). Intelligence sources say the perpetrators even gained "root level" access to some systems, a depth usually restricted to a few administrators.

After that, "we're not certain where they went," says GOP Rep. Curt Weldon, who has held classified hearings on Moonlight Maze.

As a federal interagency task force begins its damage assessment, a key question is whether the Russians managed to jump from the unclassified (although non-public) systems where they made their initial penetration into the classified Defense Department network that contains the most sensitive data. Administration officials insist the "firewalls" between the networks would have prevented any such intrusion, but other sources aren't so sure. Besides, one intelligence official admitted, classified data often lurk in unclassified databases. With enough time and computer power, the Russians could sift through their mountains of pilfered information and deduce those secrets they didn't directly steal. That's one more thing to worry about, although security officials admit that they have a more pressing concern. The intruders haven't been spotted on the network since May 14. Have they given up their efforts—or burrowed so deeply into the network that they can no longer even be traced?



DEPARTMENT OF DEFENSE